Guarding The Crown Jewels: Identifying and Stopping The Theft of Trade Secrets

February 2, 2006

Cal Bar CyberSpace Sub-Committee

Winston Krone (Safir Rosetti)

Rob Hale (Washington Mutual)

Some of this presentation was originally given in November 2005 before the San Francisco Bar Association (Barristers Club) by **Winston Krone** (SafirRosetti), **Matthew Parrella** (U.S. Department of Justice) and **Gregory Tenhoff** (Cooley Godward LLP). However, comments and opinions in the current presentation are attributable only to the current presenters.

Agenda

- The warning signs of trade secret theft
- Conducting an investigation and preserving evidence
- Advantages and disadvantages of pursuing civil vs. criminal remedies
- Initiating a criminal investigation; how to get the government involved

Warning Signs of Trade Secret Theft

The suspect:

- Had access to/ developed, key trade secrets
- Began to compete before leaving:
  - Devoting work time or equipment to new venture
  - Soliciting coworkers or customers
  - Poor work performance
- Engaged in any deception, such as:
  - Lying about the identify of new employer
  - Lying about her position with new employer

Warning Signs (continued)

- Access (print, zip, copy, or download) ANY (not just “key”) documents just prior to leaving
- Transfer information to home IP address, personal e-mail, new employer
- Insist on using own laptop/ build own computer at work/ bring in external media
- Fail or refuse to return company property

Warning Signs (continued)

- Refuse to attend an exit interview
- Attend an exit interview but fail to acknowledge contractual obligations:
  - To protect proprietary information
  - To return property
  - Not to solicit co-workers
- Refuse to identify new employer

Warning Signs (continued)

- The marketplace has given indications of improper use or disclosure – e.g. competitor announces similar offering with surprisingly fast time-to-market
- Feedback from customers
- Key Point: Theft is often not a surprise to someone in company's management

Conducting An Investigation

- Interview the reporting witnesses immediately
- Create an investigatory team
- Establish a trusted person in the IT Department
- Check your proprietary information database
- Determine which files were accessed (printed, zipped, copied, downloaded, e-mailed, etc.)
- Get the suspect's computer(s) *immediately*
  - Maintain a chain of custody
  - Preserve it in its present state
  - Make a mirror image of the hard drive

Conducting An Investigation (continued)

- Preserve server information and back-up tapes for “Network Forensics”
- Review the “data”
  - E-mails
  - Documents created by suspect
  - Lists of file activity

Conducting An Investigation (continued)

- Collect evidence of other Federal crimes (not just theft of trade secrets) – e.g.
  - unauthorized computer access
  - taking confidential information (less than trade secrets)
  - pecuniary gain

Traditional Areas of Investigation of Trade Secret Theft (non-forensic)

- Database/Background Investigations
  - Where is the suspect working?
  - Determine suspect's assets/finances
  - Has suspect/ family filed FBNs, incorporated companies, etc?
- Surveillance
- Dumpster Diving
- Employee Interviews
- Real Time Monitoring

Advantages/Disadvantages of Criminal and Civil Process

- Advantages of pursuing criminal process
  - Significantly enhanced investigation methods
    - Search warrants
    - FBI interviews of witnesses and suspects
    - Seizure of potential evidence
    - Border searches
    - Arrest/incarceration of suspects
  - Ability to interact with international law enforcement agencies

Advantages/Disadvantages (continued)

- A range of criminal statutes to pursue
- Expertise of FBI, forensic analysts, and DOJ
- No onerous civil lawsuit requirements (written disclosure of trade secrets; delays in ability to conduct discovery; limitations of discovery mechanisms; etc.)

- Disadvantages of pursuing criminal process
  - Loss of control over matter
    - Risk that FBI/DOJ will not pursue
    - No control over timing of events in the case
    - No direct control over the ultimate resolution of the case
  - Need to define value of trade secrets at early stage due to charging and plea decisions

Advantages/Disadvantages (continued)

- Clients need to be committed to seeing the process through, even if it means people go to jail – especially when the "smaller fish" are arrested

- DOJ and other law enforcement will publicize the case for deterrent purposes (but note requirement under 18 USC 1835 for courts to take such actions as necessary to preserve confidential nature of trade secrets)

Initiating A Criminal Investigation

- BEFORE contacting law enforcement:
  - Quantify the potential loss
  - Make sure it is a trade secret
  - Create a “best facts” chronology
- Approach the right branch of law enforcement and the right person

Initiating A Criminal Investigation
State –v- Federal

The greatest differences:

- **Difference in penalties**
- **Damage requirements**
- **Greater expertise and reach of Federal Law Enforcement**

Initiating A Criminal Investigation

State –v- Federal

Difference in Penalties

- **Federal**
  - **18 USC 1832 Theft of Trade Secrets**
    - **Individual – 10 years and/or up to $250K**
    - **Organization – Up to $5M**
  - **18 USC 1831 Economic Espionage**
    - **Individual – 15 years and/or up to $500K**
    - **Organization – Up to $10M.**
  - **18 USC 1030 Computer Fraud and Abuse Act**
    - **Fines and/or up to 5-10 years, depending on offense**

- **State**
  - **CA Penal Code § 499(c) – Theft of Trade Secrets**
    - **$5K and/or up to 1 year**

Initiating A Criminal Investigation

State –v- Federal

Difference in Damage Requirements

- Federal
  - 1831 (Economic Espionage) and 1832 (Theft of Trade Secrets)
    - No jurisdictional limit - the trade secret must derive "independent economic value . . . from not being generally known to . . . the public." 18 USC 1839(3)(b).
  - 1030 Computer Fraud and Abuse Act
    - No jurisdictional value for basic offence

  However, Federal law enforcement/ prosecutors have informal minimum damages of $50,000 - $150,000

- State
  - CA Penal Code § 499(c) – Theft of Trade Secrets
    - CA Sup Ct. has held that the CA Economic Crime Law of 1992 requires a mandatory minimum of 90 days imprisonment for certain offenses, including any Theft of Trade Secrets exceeding $50K in value (see *People v. Farell*)

Initiating A Criminal Investigation
State –v- Federal

Difference in Expertise/ Reach

- **Federal**
  - **Higher quality investigations and prosecutions for "high tech" crimes**
  - **Border Stops**
  - **Coordination with foreign law enforcement**
- **State**
  - **Less resources**
  - **Might be interested in smaller (i.e. less that $100k) case**

Potential Federal Crimes #1
Theft of Trade Secrets (18 USC 1832)

- Prohibits theft, possession, alteration, etc of IP w/o owner's authorization if:
  - The information is a trade secret
  - The defendant intended to convert the trade secret to the economic benefit of a non-owner
  - The defendant knew the information was proprietary
  - The defendant intended or knew that the owner would be injured
  - The trade secret was related to a product produced or intended for interstate or foreign commerce

Potential Federal Crimes #1
Theft of Trade Secrets (18 USC 1832)

Penalty

A defendant convicted for violating § 1832 can be imprisoned for up to 10 years and fined $500,000. 18 U.S.C. § 1832(a)(5). Corporations and other entities can be fined not more than $5,000,000.

Potential Federal Crimes #1
Theft of Trade Secrets (18 USC 1832)

Additional Sanctions

- The court in imposing sentencing shall order the forfeiture of any proceeds or property derived from violations of the EEA, and may order the forfeiture of any property used to commit the crime. 18 USC 1834(a)(1).

- While the EEA does not provide for civil forfeiture proceedings, it does authorize the government to file a civil action seeking injunctive relief. 18 U.S.C. § 1836(a). to prevent further disclosure of the trade secret while conducting a criminal investigation or in cases where the defendant's conduct does not warrant criminal prosecution.

Potential Federal Crimes #1
Theft of Trade Secrets (18 USC 1832)

- The term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--
  - (A) the owner thereof has taken reasonable measures to keep such information secret; and
  - (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public.

Theft of Trade Secret Case

(U.S. v. Woodard)

- Defendant was IT Director at Lightwave Microsystems (LWM)
- When LWM ceased operations, defendant stole the system backup tapes, which contained all proprietary IP
- Defendant attempted to sell tapes to LWM's competitor
- FBI alerted, UCO begun, resulting in defendant's arrest and seizure of tapes
- Defendant PG 8/1/05, to be sentenced 12/5/05

Potential Federal Crimes #2

Computer Fraud & Abuse 18 USC 1030 Obtaining Information in Excess of Authorization by Means of a Protected Computer

Alternative to 18 USC 1832

- Information does NOT need to be trade secret
- No need to prove personal gain (N.B. enhancement)
- No need to quantify loss (N.B. enhancement)

Potential Federal Crimes #2
18 USC 1030(a)(2)

Offense: Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information:

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

(B) information from any department or agency of the United States;

(C) information from any protected computer if the conduct involved an interstate or foreign communication

Potential Federal Crimes #2
18 USC 1030(a)(2)

Penalties

- **Simple violation: max 1 year imprisonment and/ or $100,000 fine.**
- **Enhanced to 5 years imprisonment/ $250,000 fine where offense committed for commercial advantage/ private financial gain OR value of information obtained exceeds $5,000.**
- **Repeat offenders: max 10 years imprisonment and/or $250,000 fine.**
- **Offenders are also subject to civil liability, 18 U.S.C. 1030(g).**
- **NOTE: All other federal conversion statutes appear to require offender either commit embezzlement by failing to comply with some fiduciary obligation or commit larceny by intending to acquire the property or to deprive another of it. 1030(a)(2) in contrast to the conversation statutes and to the computer fraud provisions of paragraph 1030(a)(4) requires no larcenous intent.**

Potential Federal Crimes #3
Economic Espionage (18 USC 1831)

Economic Espionage (18 USC 1831)

Offense:

- **(1) defendant stole, or without authorization of the owner, obtained, destroyed or conveyed information;**
- **(2) defendant knew this information was proprietary;**
- **(3) information was in fact a trade secret;**
- **(4) defendant knew offense would benefit or was intended to benefit a foreign government, foreign instrumentality, or foreign agent.**
- **(5) defendant attempts to commit any offense described above**
- **(6) defendant conspires to commit (and does an act to effect) any offense described above**

Potential Federal Crimes #3 Economic Espionage

Economic Espionage (18 USC 1831)

- *Approval Required*: Approval of Attorney General, Deputy Attorney General or Assistant Attorney General of the Criminal Division required for prosecutions brought prior to October 11, 2001; Internal Security Section coordinates requests for approval.

  Statutory maximum penalty: 15 years' imprisonment and $500,000 fine (individual); $10 million fine (corporation)

Economic Espionage Case

(U.S. v. Fei Ye, et al.)

- Pending indictment – one of only two to charge violations of 1831 – alleges that:
  - defendants allegedly stole trade secrets relating to integrated circuit design from 4 Silicon Valley cos.
  - Project allegedly known as “Supervision,” to produce and sell microprocessors for benefit of PRC
- Some of the alleged trade secrets seized from defendants at SFO

Potential Federal Crimes #4
Interstate Transport of Stolen Property

- **Interstate transportation of stolen property (18 U.S.C. 2314)**

  Federal law enforcement might use this if problems proving:

(1) existence of a trade secret;
(2) computer access was genuinely "unauthorized";
(3) foreign element (for Economic Espionage)

Potential Federal Crimes #4
Interstate Transport of Stolen Property

- **Interstate transportation of stolen property**
  (18 U.S.C. 2314)

(1) the defendant unlawfully transported or caused to be transported in interstate or foreign commerce goods, wares, or merchandise;

(2) the goods, wares, or merchandise were stolen, converted, or taken by fraud;

(3) the goods, wares, or merchandise have a value of $5,000 or more; and

(4) the defendant knew the same to be stolen, converted, or taken by fraud.

(5) Must involve a tangible item (e.g. document, computer file, etc.

(6) Receipt of stolen goods a separate offense (18 USC 2315)

Transportation of Stolen Property

Penalties

The foreign transportation of stolen property charge carries a maximum statutory penalty of 10 years imprisonment and a fine of $250,000.

Transportation of Stolen Property

(**U.S. v. Shin-Guo Tsai)** ND Cal. 2005

Tsai, a design engineer, pleaded guilty to transporting proprietary property of a Silicon Valley-based semiconductor company to a potential competitor in Taiwan. Tsai was originally arrested and charged with transporting in foreign commerce stolen "data sheets" (containing his employer's proprietary information).

In September 2005, Tsai plead guilty to this charge pursuant to a plea agreement. Tsai admitted the substance of the charges and that he had sent the stolen data sheets to a named contact in Taiwan. This gave his ex-employer the opportunity to commence legal proceedings against the Taiwanese contact.

Note: given the expedited criminal process of indictment and arrest, there were evidentiary problems with proving theft of "Trade Secrets".